HWSec: exam

R. Pacalet

2023-05-10

You can use any document but communicating devices are strictly forbidden. Please number the different pages of your paper and indicate on each page your first and last names. You can write your answers in French or in English, as you wish. Precede your answers with the question's number. If some information or hypotheses are missing to answer a question, add them. If you consider a question as absurd and thus decide to not answer, explain why. If you do not have time to answer a question but know how to, briefly explain your ideas. Note: copying verbatim the slides of the lectures or any other provided material is not considered as a valid answer. Advice: quickly go through the document and answer the easy parts first.

The first question is worth 4 points. The 3 other questions are worth 2 points each. The problem is worth 10 points.

1 Questions

1.1 Power attacks

There are different families of countermeasures against power attacks:

1. Countermeasures that increase the noise level.
2. Countermeasures that decrease the signal level.
3. Countermeasures that consist in modifying the cryptographic algorithm.
4. Countermeasures that consist in modifying the protocol around the cryptographic algorithm.

For each of these families give an example of a countermeasure that belongs to it, explain how it works, on which type of cryptographic algorithm and implementation it can be used, and discuss its benefit/cost ratio. Give an example of countermeasure that does not belong to any of these families.

1.2 Comparison of side channels

Side channel: among the different leak sources usually designated by this term there is the computation time, the power consumption and the electromagnetic emissions. Explain the advantages and drawbacks of each of these 3 side channels on an attacker's point of view.

1.3 Fault attacks

In order to protect her DES implementation against fault attacks, a security engineer decides to replace the S-boxes of the standard by carefully crafted ones and to keep them secret. What do you think of this countermeasure? Is it efficient? Is its benefit/cost ratio acceptable?

1.4 Blinding

Explain what the blinding countermeasure is, how it works, on what kind of cryptographic algorithms it can be applied, and against what types of attacks it can be used.

2 Problem: timing attack of DES decryption

To solve this problem you will need a global understanding of the DES decryption algorithm. Figure 1 should be sufficient. We remind that DES decryption is exactly the same as DES encryption with the round keys in reverse order (from K_{16} to K_1), and that only 56 bits of the 64 bits secret key are used: the 8 others are just parity bits.

- IP and FP are 64 to 64 bits permutations.
- $\oplus$ is the bitwise exclusive or.
- E is a 32 to 48 bits expansion-permutation.
- P is a 32 to 32 bits permutation.
- $S_1, S_2, \ldots, S_8$ are 8 different non-linear substitution functions with 6 bits inputs and 4 bits outputs: the S-boxes.
- PC_1 is a 64 to 56 bits selection-permutation.
- PC_2 is a 56 to 48 bits selection-permutation.
- $\ggg$ is the rotation to the right by one or two positions, depending on the round number.

All these functions are perfectly defined in the DES standard.

The famous `ACME`™ corporation designed an implementation of the DES decryption, named `acmeDESdec`™. As a security expert you are in charge of attacking `acmeDESdec`™ to evaluate its robustness against timing attacks before it can be used by the government. The IP, E, P, FP, PC_1, PC_2, $\ggg$ and $\oplus$ operations have a constant computation time but not the S-boxes: when their input is all zeros (000000) they compute their output twice faster than with the 63 other inputs. You can use `acmeDESdec`™ to decrypt as many chosen 64 bits ciphertexts as you wish and for each of them you can measure the decryption time. The timing measurements $\hat{t}$ are noisy: $\hat{t} = t + e$ where t the actual decryption time and e is a measurement error. You do **not** have access to the 64 bits decrypted plaintexts. Your goal is to retrieve the 56 useful bits of the unknown but constant secret key (we do not care about the 8 partity bits).

Explain your attack: how do you proceed, in what order and why? Carefully and clearly define your notations, express your attack algorithm in a semi-formal (pseudo-language), complete and non ambiguous way.

Is your attack practical? Does its efficiency depend on some parameters? If

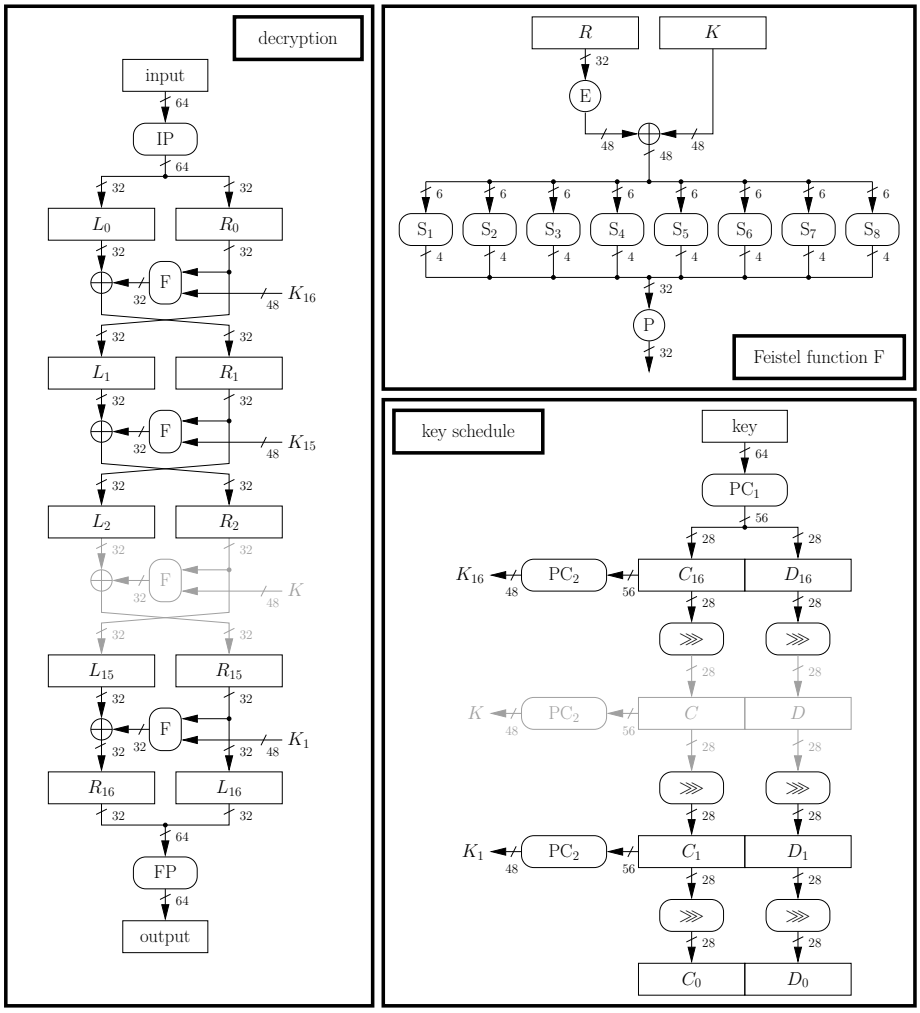

Figure 1: DES decryption

yes, what parameters? What is your opinion about `acmeDESdec`™? Is it robust against timing attacks? Do you recommend its use by the government?